Aritmética Entera

MATEMÁTICA DISCRETA I

F. Informática. UPM

Estructura de los números enteros

Definición

El conjunto de los números enteros es el conjunto

$$\mathbb{Z} = \{\ldots, -n, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, n, \ldots\}.$$

Operaciones

Definición

En $\mathbb{Z}$ se pueden definir dos operaciones binarias internas $+, \cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ con las siguientes propiedades:

i) $a+(b+c) = (a+b)+c$, $a(bc) = (ab)c$, para cualesquiera $a, b, c \in \mathbb{Z}$ (asociativa),

ii) $a+b = b+a$, $ab = ba$, para cualesquiera $a, b \in \mathbb{Z}$ (conmutativa),

iii) $a+0 = a$, $a1 = a$, para todo $a \in \mathbb{Z}$ (existencia de elemento neutro),

iv) para todo $a \in \mathbb{Z}$ existe $-a \in \mathbb{Z}$ tal que $a+(-a) = 0$ (existencia de elemento opuesto),

v) $ab = ac \Rightarrow b = c$, para cualesquiera $a, b, c \in \mathbb{Z}$ con $a \neq 0$ (cancelativa),

vi) $a(b+c) = ab+ac$, para cualesquiera $a, b, c \in \mathbb{Z}$ (distributiva).

Operaciones

Definición

En $\mathbb{Z}$ se puede definir una relación de orden total, compatible con la suma y el producto:

$$a \leq b \Rightarrow \begin{cases} a + c \leq b + c & \text{para todo } c \in \mathbb{Z} \\ ac \leq bc & \text{para todo } c \in \mathbb{Z} \text{ con } c \geq 0 \end{cases}$$

El axioma de buena ordenación

Propiedad (Axioma de buena ordenación en $\mathbb{Z}$)

Si X es un subconjunto no vacío acotado inferiormente de $\mathbb{Z}$, entonces X tiene mínimo.

Consecuencia

Si X es un subconjunto no vacío de $\mathbb{N} \cup \{0\}$, entonces X tiene mínimo.

El axioma de buena ordenación

Teorema (Principio de inducción)

Sea $S \subset \mathbb{N}$ *tal que*

i) $1 \in S$,

ii) *si* $k \in S \Rightarrow k+1 \in S$.

Entonces $S = \mathbb{N}$.

Teorema (Principio de inducción fuerte)

Sea $z_0 \in \mathbb{Z}$ *y sea* $S \subset Z_0 = \{z \in \mathbb{Z} \mid z \geq z_0\}$ *tal que*

i) $z_0 \in S$,

ii) *si* $\{z_0, z_0+1, \ldots, n\} \subset S \Rightarrow n+1 \in S$.

Entonces $S = \{z \in \mathbb{Z} \mid z \geq z_0\}$.

Divisibilidad. Teorema de la división

Definición

Dados a y b números enteros, $a \neq 0$, se dice que a divide a b $(a|b)$ si $\exists c \in \mathbb{Z}$ tal que $b = ac$. Si $a|b$ se dice que a es factor de b y que b es múltiplo de a.

Propiedades

Sean $a, b, c \in \mathbb{Z}$. Entonces

i) $1|a$,

ii) $a|0$,

iii) $a|b$ y $a|c \Rightarrow a|b+c$,

iv) $a|b$ y $a|c \Leftrightarrow a|bx+cy, \forall x, y \in \mathbb{Z}$,

v) $a|b$ y $b|a \Rightarrow a = b$ o $a = -b$.

Divisibilidad. Teorema de la división

Teorema (Teorema de la división)

Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Entonces existen $q, r \in \mathbb{Z}$ con $0 \leq r < b$ tales que $a = bq + r$. Además, q y r son únicos.
a, b, q y r se suelen llamar dividendo, divisor, cociente y resto, respectivamente.

Corolario

Sean $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$. Entonces existen $q, r \in \mathbb{Z}$, $0 \leq r < |b|$, tales que $a = bq + r$. Además, q y r son únicos.

Ejemplos

i) Si $a = 17$ y $b = 3$, $17 = 3 \cdot 5 + 2$ con $0 \leq 2 < 3$,

ii) si $a = 17$ y $b = -3$, $17 = (-3) \cdot (-5) + 2$ con $0 \leq 2 < 3 = |-3|$,

iii) si $a = -17$ y $b = 3$, $-17 = 3 \cdot (-6) + 1$ con $0 \leq 1 < 3$,

iv) si $a = -17$ y $b = -3$, $-17 = (-3) \cdot 6 + 1$ con $0 \leq 1 < 3 = |-3|$.

Demostración del Teorema de la División

Sea $R = \{x \in \mathbb{N} \cup \{0\} \mid a = by + x \text{ **para algún** } y \in \mathbb{Z}\}$.
Se tiene que $R \neq \emptyset$ pues $a = b \cdot 0 + a$ si $a \geq 0$ y $a = b \cdot a + (a - ab) = b \cdot a + a(1 - b)$ con $a(1 - b) > 0$, si $a < 0$.
Por tanto, **existe** $r = \min R \in R$ tal que $a = bq + r$ para algún $q \in \mathbb{Z}$.
Ahora, se tiene que $r < b$ pues si fuera $r - b \geq 0$, se tendría que $a = b(q + 1) + r - b$ con $0 \leq r - b < r$ (contradicción).
Vamos a ver finalmente que q **y** r **son únicos**. Supongamos que existen $q', r' \in \mathbb{Z}$ con $0 \leq r' < b$ tales que $a = bq' + r'$. Entonces $b(q' - q) = r - r'$ y por tanto, si $q < q'$ se tiene que $r = r' + b(q' - q) \geq r' + b \geq b$, y si $q > q'$ se tiene $r' = r + b(q - q') \geq r + b \geq b$. Luego ha de ser $q = q'$ y por tanto $r' = a - bq' = a - bq = r$.

Sistemas de numeración

Definición

Sea $n \in \mathbb{N}$. Se dice que n **está expresado en base 10** y se denota $n = (n_k n_{k-1} \cdots n_1 n_0)_{10}$, si $n = n_k 10^k + n_{k-1} 10^{k-1} + \cdots + n_1 10 + n_0$, con $0 \leq n_i < 10$ para todo $i \in \{0, \ldots, k\}$ y $n_k \neq 0$.
Se dice que n **está expresado en base b** $(b \geq 2)$ y se denota $n = (n_k n_{k-1} \cdots n_1 n_0)_b$ si $n = n_k b^k + n_{k-1} b^{k-1} + \cdots + n_1 b + n_0$, con $0 \leq n_i < b$ para todo $i \in \{0, \ldots, k\}$ y $n_k \neq 0$.
A la notaciones en bases 10, 2 y 16 se les llama notaciones decimal, binaria y hexadecimal.

Teorema

Sea $b \geq 2$ un número natural. Entonces todo número $n \in \mathbb{N}$ se puede expresar de forma única en la forma

$$n = n_k b^k + n_{k-1} b^{k-1} + \cdots + n_1 b + n_0, \quad k \geq 0$$

con $0 \leq n_i < b$ para todo $i \in \{0, \ldots, k\}$ y $n_k \neq 0$.

Demostración sistemas de numeración

Por el teorema de la división, $n = bq_0 + r_0$ con $0 \leq q_0 < n$ (por ser $b \leq 2$) y $0 \leq r_0 < b$.
Por otra parte $q_0 = bq_1 + r_1$ con $0 \leq q_1 < q_0 < n$ y $0 \leq r_1 < b$.
Por otra parte $q_1 = bq_2 + r_2$ con $0 \leq q_2 < q_1 < q_0 < n$ y $0 \leq r_2 < r_1 < b$.
$\vdots$
Continuando este proceso obtenemos $\{0 = q_k < q_{k-1} < \cdots < q_1 < q_0 < n\}$ y $\{r_k, r_{k-1}, \ldots, r_1, r_0\}$ tales que

$$\begin{aligned} n &= bq_0 + r_0 \\ &= b(bq_1 + r_1) + r_0 = b^2 q_1 + br_1 + r_0 = \ldots \\ &= b^2(bq_2 + r_2) + br_1 + r_0 = b^3 q_2 + b^2 q_1 + br_1 + r_0 = \ldots \\ &= b^k q_{k-1} + b^{k-1} r_{k-1} + \cdots + br_1 + r_0 \\ &= b^{k+1} q_k + b^k r_k + b^{k-1} r_{k-1} + \cdots + br_1 + r_0 \\ &= b^k r_k + b^{k-1} r_{k-1} + \cdots + br_1 + r_0. \end{aligned}$$

Demostración sistemas de numeración

Para probar que esta expresión es única, supongamos que

$$n = b^k r_k + b^{k-1} r_{k-1} + \cdots + b r_1 + r_0 = b^s r'_s + b^{s-1} r'_{S-1} + \cdots + b r'_1 + r'_0$$

con $0 \leq r_i < b$ para todo $i \in \{0, \ldots, k\}$ y $b_k \neq 0$, $0 \leq r'_i < b$ para todo $i \in \{0, \ldots, s\}$ y $n_k \neq 0$.
Supongamos que $s \leq k$ y definamos $r'_i = 0$ si $s < i \leq k$. Entonces

$$n = b^k r_k + b^{k-1} r_{k-1} + \cdots + b r_1 + r_0 = b^k r'_k + b^{k-1} r'_{k-1} + \cdots + b r'_1 + r'_0$$

y por tanto $b^k(r'_k - r_k) + b^{k-1}(r'_{k-1} - r_{k-1}) + \cdots + b(r'_1 - r_0) + (r'_0 - r_0) = 0$.
Por tanto $b|(r'_0 - r_0)$ y como $0 \leq |r_0 - r'_0| < b$ (por ser $0 \leq r_0, r'_0 < b$), entonces $r_0 = r'_0$. Además, entonces se tiene que $b^k(r'_k - r_k) + b^{k-1}(r'_{k-1} - r_{k-1}) + \cdots + b(r'_1 - r_0) = 0$.
Por tanto $b^{k-1}(r'_k - r_k) + b^{k-2}(r'_{k-1} - r_{k-1}) + \cdots + (r'_1 - r_0) = 0$ y razonando igual que antes se tiene que $r_1 = r'_1$.
Continuando el proceso se obtiene que $r_i = r'_i$ para todo $i \in \{0, \ldots, k\}$.
Finalmente, como $r_k \neq 0$, entonces $r'_k \neq 0$ y por tanto $s = k$.

El máximo común divisor

Definición

Dados $a, b \in \mathbb{Z} \setminus \{0\}$ se dice que $d \geq 1$ es el máximo comun divisor de a y b si $d|a$, $d|b$ y cualquier otro $c \in \mathbb{Z}$ tal que $c|a$, $c|b$ verifica que $c|d$.

Observación

Dados $a, b \in \mathbb{Z} \setminus \{0\}$ existe un único $d \geq 1$ tal que d es el máximo comun divisor de a y b. Se denota $d = \mathrm{mcd}(a, b)$.

Teorema

Sean $a, b \in \mathbb{Z} \setminus \{0\}$ y sea $d = \mathrm{mcd}(ab)$. Entonces d es el menor entero positivo no nulo que puede expresarse en la forma $ax + by$ con $x, y \in \mathbb{Z}$.

El máximo común divisor

Definición

Dados $a, b \in \mathbb{Z} \setminus \{0\}$ se dice que $d \geq 1$ es el máximo comun divisor de a y b si $d|a$, $d|b$ y cualquier otro $c \in \mathbb{Z}$ tal que $c|a$, $c|b$ verifica que $c|d$.

Observación

Dados $a, b \in \mathbb{Z} \setminus \{0\}$ existe un único $d \geq 1$ tal que d es el máximo comun divisor de a y b. Se denota $d = \mathrm{mcd}(a, b)$.

Teorema

Sean $a, b \in \mathbb{Z} \setminus \{0\}$ y sea $d = \mathrm{mcd}(ab)$. Entonces d es el menor entero positivo no nulo que puede expresarse en la forma $ax + by$ con $x, y \in \mathbb{Z}$.

Corolario

Sean $a, b \in \mathbb{Z} \setminus \{0\}$. Entonces $\mathrm{mcd}(a, b) = 1$ si y solo si existen $s, t \in \mathbb{Z}$ tales que $as + bt = 1$. Se dice en este caso que a y b son primos entre sí.

El máximo común divisor

Propiedades

Sean $a, b \in \mathbb{Z}$. Entonces

i) $\mathrm{mcd}(a, b) = \mathrm{mcd}(|a|, |b|)$,

ii) $\mathrm{mcd}(ka, kb) = |k| \,\mathrm{mcd}(a, b)$,

iii) $\mathrm{mcd}(a, b) = d \Leftrightarrow d|a, d|b$ y $\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

El algoritmo de Euclides

Proposición

Sean $a, b \in \mathbb{Z} \setminus \{0\}$. *Entonces* $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$ *donde* r *es el resto de la división de* a *por* b.

Observación (Algoritmo de Euclides)

Sean $a, b \in \mathbb{N}$ con $a \geq b > 0$. Entonces $a = bq_1 + r_1$ con $0 \leq r_1 < b$, donde si $r_1 = 0$ se tiene que $\mathrm{mcd}(a, b) = b$. Si $r_1 \neq 0$ se tiene que $b = r_1 q_2 + r_2$ con $r_2 < r_1$, donde si $r_2 = 0$ se tiene que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = r_1$. Si $r_2 \neq 0$ se tiene que $r_1 = r_2 q_3 + r_3$ con $r_3 < r_2$, donde si $r_3 = 0$ se tiene que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = r_2$. De esta forma, continuando el proceso, obtenemos $\{0 = r_k < r_{k-1} < \cdots < r_2 < r_1 < b\}$. Pero entonces, como $r_{k-2} = r_{k-1} q_k + r_k = r_{k-1} q_k$, se tiene que

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \cdots = r_{k-1}.$$

Ecuaciones diofánticas de primer grado

Lema (Lema de Euclides)

Sean $a, b, c \in \mathbb{Z}$ *con* $\mathrm{mcd}(a, b) = 1$ *tales que* $a|bc$. *Entonces* $a|c$.

Teorema

La ecuación diofántica $ax + by = c$, *con* $a, b, c \in \mathbb{Z} \setminus \{0\}$ *tiene soluciones enteras si y solo si* $d = \mathrm{mcd}(a, b)|c$. *Además, en este caso, su solución general es de la forma*

$$\left\{ \begin{array}{l} x = x_1 + \dfrac{tb}{d} \\ \\ y = y_1 - \dfrac{ta}{d} \end{array} \right\} \text{ para todo } t \in \mathbb{Z}$$

donde (x_1, y_1) *es una solución particular de* $ax + by = c$ *(por ejemplo la que se obtiene a partir del algoritmo de Euclides).*

Números primos

Definición

Diremos que un número entero $p > 1$ es primo si sus únicos divisores positivos son 1 y p. Si p no es primo se dice que es compuesto. Por tanto, q es compuesto si y solo si existen $a, b \in \{2, 3, \ldots, n-1\}$ tales que $q = ab$. Diremos que p y q son primos entre sí si $\mathrm{mcd}(p, q) = 1$.

Teorema

Sea $p > 1$, p primo, tal que $p|ab$, $a, b \in \mathbb{Z}$. Entonces $p|a$ o $p|b$.

Corolario

Sea $p > 1$, p primo tal que $p|p_1 p_2 \cdots p_n$ con $p_1, p_2, \ldots, p_n \in \mathbb{Z}$. Entonces existe $i \in \{1, 2, \ldots, n\}$ tal que $p|p_i$.

Números primos

Teorema (Teorema Fundamental de la Aritmética)

Todo número natural $n > 1$ o bien es primo, o puede expresarse de forma única (salvo el orden de los factores) como producto de números primos.

Observación

Si un número n es compuesto, entonces ha de tener un divisor primo menor o igual que $\sqrt{n}$.

Teorema

Existen infinitos números primos.

Observación

El método más antiguo y conocido de obtener todos los números primos menores que un entero dado n es la criba de Eratóstenes. Por la observación anterior, solamente es necesario hacer la criba empezando por los números menores que $\sqrt{n}$.